STATE SECURITY STANDARDS FOR PERSONAL INFORMATION

2013 GENERAL SESSION

STATE OF UTAH

LONG TITLE

General Description:

This bill amends the Medical Assistance Act to require a health care provider to give a patient notice that some personal identifying information about the patient may be shared with the state's Medicaid and Children's Health Insurance Program eligibility database, and amends provisions in the Utah Technology Governance Act related to statewide security standards for personal information stored or transmitted on state servers.

Highlighted Provisions:

This bill:

- beginning July 1, 2013, requires a health care provider who participates in the state Medicaid program or the Children's Health Insurance Program to include in the health care provider's notice of privacy practices that the health care provider either has, or may submit personally identifiable information about the patient to the state's Medicaid and Children's Health Insurance Program eligibility database;
- requires the state Medicaid program and Children's Health Insurance Program, before giving a provider access to the state's eligibility database, to verify that the health care provider's notice of privacy practices complies with federal and state law;
- gives the Department of Health administrative rulemaking authority to establish uniform language for the state requirement for the notice of privacy practices to patients;
- amends the Utah Technology Governance Act to require the state's chief information officer to:
  - in coordination with the governor's office, convene a group of experts to identify industry best practices for data security standards;

- incorporate industry best practices for data security standards into the Department of Technology Services and executive branch agency practices;
- modify the state's executive branch information technology strategic plan to incorporate the industry best practices standards, as feasible within the Department of Technology Services or executive branch agency budgets;
- inform the speaker of the House of Representatives and the president of the Senate if security standards are not adopted due to budget issues; and
- conduct an assessment of the Department of Technology Services and executive branch agency security standards at least once every two years;

▸ provides a process in which a state agency that contracts for services from the Department of Technology Services may enter into an agreement with the department to audit the security standards implemented by the department; and

▸ makes technical and conforming amendments

Money Appropriated in this Bill:

None

Other Special Clauses:

None

Utah Code Sections Affected:

AMENDS:

63F-1-104, as last amended by Laws of Utah 2011, Chapter 270

63F-1-202, as last amended by Laws of Utah 2010, Chapter 286

63F-1-203, as last amended by Laws of Utah 2011, Chapter 270

63F-1-204, as last amended by Laws of Utah 2008, Chapter 382

63F-1-604, as last amended by Laws of Utah 2011, Chapter 270

ENACTS:

26-18-17, Utah Code Annotated 1953

Be it enacted by the Legislature of the state of Utah:

Section 1. Section **26-18-17** is enacted to read:

26-18-17. Patient notice of health care provider privacy practices.

(1) (a) For purposes of this section:

(i) "Health care provider" means a health care provider as defined in Section 78B-3-403 who:

(A) receives payment for medical services from the Medicaid program established in this chapter, or the Children's Health Insurance Program established in Chapter 40, Utah Children's Health Insurance Act; and

(B) submits a patient's personally identifiable information to the Medicaid eligibility database or the Children's Health Insurance Program eligibility database.

(ii) "HIPAA" means 45 C.F.R. Parts 160, 162, and 164, Health Insurance Portability and Accountability Act of 1996, as amended.

(b) Beginning July 1, 2013, this section applies to the Medicaid program, the Children's Health Insurance Program created in Chapter 40, Utah Children's Health Insurance Act, and a health care provider.

(2) A health care provider shall, as part of the notice of privacy practices required by HIPAA, provide notice to the patient or the patient's personal representative that the health care provider either has or may submit personally identifiable information about the patient to the Medicaid eligibility database and the Children's Health Insurance Program eligibility database.

(3) The Medicaid program and the Children's Health Insurance Program may not give a health care provider access to the Medicaid eligibility database or the Children's Health Insurance Program eligibility database unless the health care provider's notice of privacy practices complies with Subsection (2).

(4) The department may adopt an administrative rule to establish uniform language for the state requirement for the notice of privacy practices to patients required under Subsection (2).

Section 2. Section **63F-1-104** is amended to read:

63F-1-104. Purposes.

The department shall:

(1) lead state executive branch agency efforts to reengineer the state's information technology architecture with the goal of coordinating central and individual agency information technology in a manner that:

(a) ensures compliance with the executive branch agency strategic plan; and

(b) ensures that cost-effective, efficient information and communication systems and

resources are being used by agencies to:

(i) reduce data, hardware, and software redundancy;

(ii) improve system interoperability and data accessibility between agencies; and

(iii) meet the agency's and user's business and service needs;

(2) [~~(a)~~] coordinate an executive branch strategic plan for all agencies;

[~~(b)~~] (3) each year, in coordination with the governor's office, convene a group of public and private sector information technology and data security experts to identify best practices from agencies and other public and private sector entities[~~; and~~], including best practices for data and information technology system security standards;

[~~(c)~~] (4) develop and implement processes to replicate information technology best practices and standards identified in Subsection (3), throughout the executive branch;

(5) by December 1, 2014, and at least once every two years thereafter:

(a) evaluate the adequacy of the department's and the executive branch agencies' data and information technology system security standards through an independent third party assessment; and

(b) communicate the results of the independent third party assessment to the appropriate executive branch agencies and to the president of the Senate and the speaker of the House of Representatives;

[~~(3)~~] (6) oversee the expanded use and implementation of project and contract management principles as they relate to information technology projects within the executive branch;

[~~(4)~~] (7) serve as general contractor between the state's information technology users and private sector providers of information technology products and services;

[~~(5)~~] (8) work toward building stronger partnering relationships with providers;

[~~(6)~~] (9) develop service level agreements with executive branch departments and agencies to ensure quality products and services are delivered on schedule and within budget;

[~~(7)~~] (10) develop standards for application development including a standard methodology and cost-benefit analysis that all agencies shall utilize for application development activities;

[~~(8)~~] (11) determine and implement statewide efforts to standardize data elements and determine data ownership assignments among executive branch agencies;

[~~(9)~~] (12) develop systems and methodologies to review, evaluate, and prioritize existing information technology projects within the executive branch and report to the governor and the Public Utilities and Technology Interim Committee on a semiannual basis regarding the status of information technology projects; and

[~~(10)~~] (13) assist the Governor's Office of Planning and Budget with the development of information technology budgets for agencies.

Section 3. Section **63F-1-202** is amended to read:

63F-1-202. Technology Advisory Board -- Membership -- Duties.

(1) There is created the Technology Advisory Board to the chief information officer. The board shall have seven members as follows:

(a) three members appointed by the governor who are individuals actively involved in business planning for state agencies;

(b) one member appointed by the governor who is actively involved in business planning for higher education or public education;

(c) one member appointed by the speaker of the House of Representatives and president of the Senate from the Legislative Automation Committee of the Legislature to represent the legislative branch;

(d) one member appointed by the Judicial Council to represent the judicial branch; and

(e) one member appointed by the governor who represents private sector business needs in the state, but who is not an information technology vendor for the state.

(2) (a) The members of the advisory board shall elect a chair from the board by majority vote.

(b) The department shall provide staff to the board.

(c) (i) A majority of the members of the board constitutes a quorum.

(ii) Action by a majority of a quorum of the board constitutes an action of the board.

(3) The board shall meet as necessary to advise the chief information officer and assist the chief information officer and executive branch agencies in coming to consensus on:

(a) the development and implementation of the state's information technology strategic plan;

(b) critical information technology initiatives for the state;

(c) the development of standards for state information architecture;

(d) identification of the business and technical needs of state agencies;

(e) the department's performance measures for service agreements with executive branch agencies and subscribers of services, including a process in which an executive branch agency may review the department's implementation of and compliance with an executive branch agency's data security requirements; and

(f) the efficient and effective operation of the department.

(4) A member may not receive compensation or benefits for the member's service, but may receive per diem and travel expenses in accordance with:

(a) Section 63A-3-106;

(b) Section 63A-3-107; and

(c) rules made by the Division of Finance pursuant to Sections 63A-3-106 and 63A-3-107.

Section 4. Section **63F-1-203** is amended to read:

63F-1-203. Executive branch information technology strategic plan.

(1) In accordance with this section, the chief information officer shall prepare an executive branch information technology strategic plan:

(a) that complies with this chapter; and

(b) which shall include:

(i) a strategic plan for the:

(A) interchange of information related to information technology between executive branch agencies;

(B) coordination between executive branch agencies in the development and maintenance of information technology and information systems, including the coordination of agency information technology plans described in Section 63F-1-204; and

(C) protection of the privacy of individuals who use state information technology or information systems, including the implementation of industry best practices for data and system security that are identified in Subsection 63F-1-104(3);

(ii) priorities for the development and implementation of information technology or information systems including priorities determined on the basis of:

(A) the importance of the information technology or information system; and

(B) the time sequencing of the information technology or information system; and

(iii) maximizing the use of existing state information technology resources.

(2) In the development of the executive branch strategic plan, the chief information officer shall consult with:

(a) all cabinet level officials [~~and~~];

(b) the advisory board created in Section 63F-1-202[~~.~~]; and

(c) the group convened in accordance with Subsection 63F-1-104(3).

(3) (a) Unless withdrawn by the chief information officer or the governor in accordance with Subsection (3)(b), the executive branch strategic plan takes effect 30 days after the day on which the executive branch strategic plan is submitted to:

(i) the governor; and

(ii) the Public Utilities and Technology Interim Committee.

(b) The chief information officer or the governor may withdraw the executive branch strategic plan submitted under Subsection (3)(a) if the governor or chief information officer determines that the executive branch strategic plan:

(i) should be modified; or

(ii) for any other reason should not take effect.

(c) The Public Utilities and Technology Interim Committee may make recommendations to the governor and to the chief information officer if the commission determines that the executive branch strategic plan should be modified or for any other reason should not take effect.

(d) Modifications adopted by the chief information officer shall be resubmitted to the governor and the Public Utilities and Technology Interim Committee for their review or approval as provided in Subsections (3)(a) and (b).

(4) (a) The chief information officer shall, on or before January 1, 2014, and each year thereafter, modify the executive branch information technology strategic plan to incorporate security standards that:

(i) are identified as industry best practices in accordance with Subsections 63F-1-104(3) and (4); and

(ii) can be implemented within the budget of the department or the executive branch agencies.

(b) The chief information officer shall inform the speaker of the House of

Representatives and the president of the Senate on or before January 1 of each year if best practices identified in Subsection (4)(a)(i) are not adopted due to budget issues considered under Subsection (4)(a)(ii).

[~~(4)~~] (5) The executive branch strategic plan is to be implemented by executive branch agencies through each executive branch agency adopting an agency information technology plan in accordance with Section 63F-1-204.

Section 5. Section **63F-1-204** is amended to read:

63F-1-204. Agency information technology plans.

(1) (a) By July 1 of each year, each executive branch agency shall submit an agency information technology plan to the chief information officer at the department level, unless the governor or the chief information officer request an information technology plan be submitted by a subunit of a department, or by an executive branch agency other than a department.

(b) The information technology plans required by this section shall be in the form and level of detail required by the chief information officer, by administrative rule adopted in accordance with Section 63F-1-206, and shall include, at least:

(i) the information technology objectives of the agency;

(ii) any performance measures used by the agency for implementing the agency's information technology objectives;

(iii) any planned expenditures related to information technology;

(iv) the agency's need for appropriations for information technology;

(v) how the agency's development of information technology coordinates with other state and local governmental entities;

(vi) any efforts the agency has taken to develop public and private partnerships to accomplish the information technology objectives of the agency; [~~and~~]

(vii) the efforts the executive branch agency has taken to conduct transactions electronically in compliance with Section 46-4-503[~~.~~]; and

(viii) the executive branch agency's plan for the timing and method of verifying the department's security standards, if an agency intends to verify the department's security standards for the data that the agency maintains or transmits through the department's servers.

(2) (a) Except as provided in Subsection (2)(b), an agency information technology plan described in Subsection (1) shall comply with the executive branch strategic plan established in

accordance with Section 63F-1-203.

(b) If the executive branch agency submitting the agency information technology plan justifies the need to depart from the executive branch strategic plan, an agency information technology plan may depart from the executive branch strategic plan to the extent approved by the chief information officer.

(3) (a) On receipt of a state agency information technology plan, the chief information officer shall forward a complete copy of the agency information technology plan to the Division of Enterprise Technology created in Section 63F-1-401 and the Division of Integrated Technology created in Section 63F-1-501.

(b) The divisions shall provide the chief information officer a written analysis of each agency plan submitted in accordance with [~~Sections~~] Subsections 63F-1-404(14) and 63F-1-504(3).

(4) (a) The chief information officer shall review each agency plan to determine:

(i) (A) whether the agency plan complies with the executive branch strategic plan and state information architecture; or

(B) to the extent that the agency plan does not comply with the executive branch strategic plan or state information architecture, whether the executive branch entity is justified in departing from the executive branch strategic plan, or state information architecture; and

(ii) whether the agency plan meets the information technology and other needs of:

(A) the executive branch agency submitting the plan; and

(B) the state.

(b) In conducting the review required by Subsection (4)(a), the chief information officer shall consider the analysis submitted by the divisions under Subsection (3).

(5) After the chief information officer conducts the review described in Subsection (4) of an agency information technology plan, the chief information officer may:

(a) approve the agency information technology plan;

(b) disapprove the agency information technology plan; or

(c) recommend modifications to the agency information technology plan.

(6) An executive branch agency or the department may not submit a request for appropriation related to information technology or an information technology system to the governor in accordance with Section 63J-1-201 until after the executive branch agency's

information technology plan is approved by the chief information officer.

Section 6. Section **63F-1-604** is amended to read:

63F-1-604. Duties of the division.

The division shall:

(1) be responsible for providing support to executive branch agencies for an agency's information technology assets and functions that are unique to the executive branch agency and are mission critical functions of the agency;

(2) conduct audits of an executive branch agency when requested under the provisions of Section 63F-1-208;

(3) conduct cost-benefit analysis of delegating a department function to an agency in accordance with Section 63F-1-208;

(4) provide in-house information technology staff support to executive branch agencies;

(5) establish accountability and performance measures for the division to assure that the division is:

(a) meeting the business and service needs of the state and individual executive branch agencies; and

(b) implementing security standards in accordance with Subsection 63F-1-203(4);

(6) establish a committee composed of agency user groups for the purpose of coordinating department services with agency needs;

(7) assist executive branch agencies in complying with the requirements of any rule adopted by the chief information officer; and

(8) by July 1, [~~2006~~] 2013 and each July 1 thereafter, report to the Public Utilities and Technology Interim Committee on the performance measures used by the division under Subsection (5) and the results.